*-*Получив просьбу дать в долг, положить деньги на телефон, заплатить за Интернет... перезвоните и уточните, действительно ли знакомый нуждается в деньгах. Если у вас нет его номера, подумайте, стал бы этот человек просить у вас денег?

         - При получении sms - просьб, в том числе в социальных сетях (Вконтакте, Одноклассники, Facebook, Instagram, Viber, WhatsApp, Telegram и др.) от родственников или «друга», о переводе денежных средств, о передаче реквизитов банковской карты, либо логина и пароля для входа в кабинет Интернет-банкинга, мобильного банкинга, либо иной просьбы, связанной с денежными средствами, в первую очередь, успокойтесь и попробуйте связаться с этим человеком по имеющемуся у вас номеру. Если не отвечает - подождите немного или позвоните знакомым этого человека.

         - В банкомате, да и любым другим способом, вы можете перевести деньги только со своей карты на чужую. Перевод наоборот, с чужой карты или счета - на вашу карту, невозможен. Если вас убеждают в обратном - это ложь.

         - Помните, что операции по карте, платежи и переводы в Интернет-банке, мобильном банке НЕЛЬЗЯ отменить. Тем более, не существует никаких кодов для отмены операции или кодов «подтверждения отмены».

         - Ни в коем случае не сообщайте третьим лицам, даже если они представляются сотрудниками банка или другой финансовой организации, персональные данные или информацию о банковской карте (ПИН, CVV - код, срок действия, код 3D - Secure).

         - Если ваша банковская карта поддерживает код 3D - Secure, обязательно установите его.

         - Подключите услугу sms-информирования (оповещения). С помощью этой услуги вы получаете возможность узнать о несанкционированных операциях с вашей картой, поскольку все данные о расходах фиксируются в режиме реального времени, что позволяет повысить безопасность при использовании карты.

         - В случае утери банковской пластиковой карты, лучше немедленно произвести ее блокировку. Если реквизиты банковской карты стали известны другим лицам, велика вероятность хищения денежных средств, находящихся на счете.

         - Переводите деньги за товары только проверенным магазинам, либо физическим лицам и только после того, как вы убедитесь в наличии товара.

***Как защитить страницу в социальной сети «Вконтакте»?***

         1. Используйте сложный пароль. Хороший пароль состоит минимум из 8 символов и сочетает в себе и буквы, и цифры. Используйте разные пароли для страницы Вконтакте, почтового ящика и остальных сайтов. Секреты хорошего пароля:

         - избегайте слов из словарей, повторяющихся и идущих подряд на клавиатуре символов (iloveyou, 44444, олджэ).

         - не используйте общеизвестные данные: даты рождения, фамилии, номера машин, документов и их комбинации.

         - буквы в пароле не должны идти в алфавитном порядке. Пароль sdjyriekaoza лучше, чем acfknoswz.

         - пароль обязательно должен содержать цифры, а также большие и маленькие буквы. Пароль jaTp0rThs лучше пароля jatportgs.

         2. Следите, чтобы страница была привязана к актуальному номеру телефона и почтовому ящику. Никогда и никому не сообщайте коды, которые Вы получили от нас по SMS/

         3. Периодически проверяйте историю активности страницы. Найти её можно по адресу: https://vk/com/settings?act=security. В разделе «Безопасность» нажмите на «Показать историю активности», если заметите там что-то подозрительное (незнакомый IP, браузер, время захода) - немедленно нажимайте на «Завершить все сеансы» и меняйте пароли.

         4. Не устанавливайте программы, расширяющие функционал сайта. Например, для скачивания музыки или для изменения внешнего вида страниц Вконтакте. Зачастую мошенники распространяют через них вирусы, с помощью которых потом взламывают Вашу страницу. Также не используйте мошеннические сервисы для «накрутки» чего бы то ни было у нас на сайте.

         5. Не переходите по сомнительным ссылкам и нигде не вводите данные для входа на свою страницу. «Гости страницы», «Бесплатные голоса», «Просмотр скрытой информации» - все подобные сайты создают злоумышленники, желая или списать деньги с Вашего счёта, или получить доступ к Вашей странице. Будьте бдительны.

         6. Обязательно обзаведитесь антивирусом и регулярно проверяйте свой компьютер. Если пока полноценного антивируса у Вас нет, в качестве временного решения вы можете запустить антивирусный Cezurity. Подробнее прочитать о нем можно здесь. Если Вы пользуетесь устройством на Android. рекомендуем проверить его этим антивирусом: https://vk/cc/4ctXJ3.

         В качестве закрепления усвоенного материала предлагаем Вам пройти небольшой тест: https://vk/com/test

         Если Вы будете следовать этим простым правилам с Вашей страницей всё будет в порядке.

***Двухфакторная аутентификация страницы «Вконтакте»***

***Подключение дополнительного способа проверки.***

         Активировать функцию можно в меню «Настройки» на вкладке «Безопасность». В группе настроек «Подтверждение входа» следует нажать кнопку «Подключить».

         Подтверждение входа добавляет новый уровень проверки при авторизации на сайте. Чтобы попасть на страницу, становится недостаточно указать верные логин и пароль, необходимо также ввести специальный код подтверждения.

         Вы можете получить код подтверждения с помощью бесплатного SMS на привязанный к Вашей странице мобильный номер либо настроить и использовать специальное приложение для смартфона. Также рекомендуется распечатать список резервных кодов, чтобы можно было воспользоваться ими, если с мобильным телефоном что-то произойдёт.

         Код подтверждения действует только один раз, поэтому даже если Ваш логин, пароль и использованный код подсмотрят или перехватят, с их помощью всё равно не получится зайти на страницу.

         Проверка неутомительна: при авторизации Вы можете запомнить данный браузер, после этого для входа с него будет достаточно ввести логин и пароль, код больше не потребуется.

         В любой момент Вы сможете снять подтверждение на всех устройствах либо только на текущем. Тогда при следующей попытке авторизоваться система запросит код подтверждения повторно.

         Если кто-то попытается зайти на Вашу страницу, Вы получаете всплывающее оповещение об этом.

         Подтверждение входа защити Вас также и от возможного увода страницы в случае кражи SIM-карты. Если дополнительное подтверждение подключено, то вместо быстрого восстановления пароля, по SMS будет применяться восстановление пароля на e-mail. Таким образом, чтобы получить доступ к странице, взломщику нужно будет одновременно украсть Вашу SIM-карту, а также узнать логин и пароль от личной страницы либо от почтового ящика.

         Сделать эти вещи одновременно практически невозможно.

         Если Вы сами забудете пароли от страницы и почты или потеряете мобильный телефон и резервные коды, единственной возможностью вернуть доступ к странице станет форма восстановления доступа. Поэтому лучше всего оформить Вашу страницу в соответствии с правилами сайта: указать на ней свои истинные имя и фамилию и загрузить настоящие фотографии в качестве главных. В противном случае администрация сайта не сможет вернуть её Вам, чтобы обеспечить запрошенный уровень безопасности.